UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/960,610 | 09/21/2001 | Richard B. LeVine | ECD-0012 | 5654 |

7590 12/08/2006

Mills & Onello LLP
Suite 605
Eleven Beacon Street
Boston, MA 02108

| EXAMINER | |
|---|---|
| BESROUR, SAOUSSEN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | |

DATE MAILED: 12/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/960,610 | LEVINE ET AL. | |
| | Examiner | Art Unit | |
| | Saoussen Besrour | 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *21 September 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *See Continuation Sheet* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,11-30,32,57,59-63,85-87,89-92,98-116,118-127,129-133,155-157,159 and 161-183* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This action is in response to amendment filed 9/21/2006. Claims 1, 29, 56, 59, 61, 85, 89, 111, 112, 115, 126, 129, 131, 155 and 159 were amended. Claims 6-10, 31, 58, 64-84, 88, 93-97, 117, 128, 134-154, 158 and 160 were cancelled. New claims 161-174 were added. Claims 1-5, 11-30, 32, 57, 59-63, 85-87, 89-92, 98-116, 118-127, 129-133, 155-157, 159, and 161-183 are pending.

### *Allowable Subject Matter*

2. The indicated allowability of claims 1, 29, 56, 85, 89, 115, 126, 155 and 159 is withdrawn in view of the newly discovered reference(s) to Weidong (U.S. Patent No. 6,819,766), Xu et al. (U.S. Pub. No. 2006/0053307), and Attalah et al. (U.S. Pub. No. 2006/0031686). Rejections based on the newly cited reference(s) follow.

### *Claim Objections*

3. **Claims 24 and 51** objected to because of the following informalities: replace "if" with "when". Appropriate correction throughout the claims is required.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1, 2, 3, 4, 5, 11, 12, 13, 14, 20, 25, 26, 89, 90, 91, 92, 98, 99, 100, 101, 107, 11 and 112** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Weidong (U.S. Patent No. 6,819,766).

As per **claim 1**, Reitmeier et al. discloses: subdividing the digital content data into data segments ([0023]); modifying the data segments with second data to generate modified data ([0029]); and storing the modified data at predetermined memory locations ([0036]); encrypting the modified data and storing the encrypted modified data (Paragraph 31, Lines 1-4); encrypting the modified data with an encryption key (Paragraph 57, Lines 1-9). Reitmeier et al. does not explicitly teach encrypting the encryption key; storing the encryption key with the encrypted modified data at the predetermined memory locations; and partitioning the encryption key among the encrypted modified data. However, Weidong discloses: encrypting the encryption key (Column 2, Lines 48); storing the encryption key with the encrypted modified data at the predetermined memory locations (Column 2, Lines 50-60); and partitioning the encryption key among the encrypted modified data (Column 2, Lines 50-60). Weidong further provides the motivation that this method is capable of encryption key management without requiring security infrastructure such as a key distribution center or a certificate authority (Column 2, Lines 30-33). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Weidong in conjunction with the teachings of Reitmeier et al. for the benefit

of managing encryption keys for encrypted data without requiring a security infrastructure.

As per **claim 89**, Reitmeier et al. discloses: a subdividing unit (segmentation module) for subdividing the digital content data into data segments (figure 1, item 110A, [0023]); a modification unit (re-sequencing module) for modifying the data segments with second data to generate modified data (figure 1, item 130, [0029]); a storage unit for storing the modified data at predetermined memory locations (figure 1, item 155, [0036]); an encryption unit for encrypting the modified data and storing the encrypted modified data, wherein the encryption unit further encrypts the modified data with an encryption key (Paragraph 31, Lines 1-4 and Paragraph 57, lines 1-9). Reitmeier et al. does not explicitly teach wherein the encryption unit further encrypts the encryption key, and wherein the storage unit further stores the encryption key with the encrypted modified data at the predetermined memory location (Column 2, Lines 50-60); and a partitioning unit for partitioning the encrypted key among the encrypted modified data (Column 2, Lines 48-60). Weidong further provides the motivation that this method is capable of encryption key management without requiring security infrastructure such as a key distribution center or a certificate authority (Column 2, Lines 30-33). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Weidong in conjunction with the teachings of Reitmeier et al. for the benefit of managing encryption keys for encrypted data without requiring a security infrastructure.

As per **claim 2**, rejected as applied to claim 1. Furthermore, Reitmeier discloses: data types selected from a group consisting of audio, video, documents, text and software (Paragraph 16).

As per **claims 3 and 90**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: the data segments are of a variable length (Paragraph 29).

As per **claims 4 and 91**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: the second data comprises a randomly generated data stream (Paragraph 29).

As per **claims 5 and 92**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: the second data comprises portions of the digital content data (Paragraph 29).

As per **claims 11 and 98**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: the predetermined memory locations are selected as the locations at which the digital content data was originally stored (Paragraph 29).

As per **claims 12 and 99**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored (Paragraph 29).

As per **claims 13 and 100**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: generating a map of locations at which the modified data is stored (Paragraph 18, index table).

As per **claims 14 and 101**, rejected as applied to claims 13 and 100. Furthermore, Reitmeier et al. discloses: storing the map of locations at the predetermined memory locations (Paragraph 18 and Paragraph 36).

As per **claims 20 and 107**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: retrieving the modified data from the predetermined memory locations; and de-interleaving the data segments based on the second data to generate original digital content data (Fig 4, Paragraph 46).

As per **claims 25 and 111**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data (Paragraph 57).

As per **claims 26 and 112**, rejected as applied to claims 1 and 89. Furthermore, Reitmeier et al. discloses: modifying the data segments with second data comprises tokenizing the data segments with token data (Paragraph 31, encryption in electronic codebook mode).

5. **Claims 15, 16, 17, 18, 19, 21, 22, 23, 24, 102, 103, 104, 105, 106, 108, 109 and 100** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Weidong (U.S. Patent No. 6,819,766) in further view of Jensen et al. (US Patent No. 5,930,828).

As per **claims 15 and 102**, rejected as applied to claims 1 and 89. The combined references Reitmeier et al. and Weidong substantially teach subdividing the digital content data into data segments; modifying the data segments with second data

to generate modified data; and storing the modified data at predetermined memory locations; encrypting the modified data and storing the encrypted modified data; encrypting the modified data with an encryption key; encrypting the encryption key; storing the encryption key with the encrypted modified data at the predetermined memory locations; and partitioning the encryption key among the encrypted modified data. The combined teachings of Reitmeier et al. and Weidong do not explicitly disclose the memory locations reside on a system and further comprising: scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data. However, Jensen et al. discloses: the memory locations reside on a system and further comprising: scanning the system to determine available memory locations (Column 12, Lines 13-19); selecting target memory locations within the available memory locations at which to store the modified data (Column 12, Lines 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanning and targeting of Jensen et al. with the combined teachings of Reitmeier et al. and Weidong to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claims 16 and 103**, rejected as applied to claims 15 and 102. The combined references Reitmeier et al., Weidong and Jensen et al. substantially teach the memory locations reside on a system and further comprising: scanning the system to

determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations. Furthermore, Jensen et al. discloses: a subset of available memory locations are located within file system locations (Column 3, Lines 55-61). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the teachings of Jensen et al. with the combined teachings of Reitmeier et al. and Weidong to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claims 17 and 104**, rejected as applied to claims 15 and 102. The combined references Reitmeier et al., Weidong and Jensen et al. substantially teach the memory locations reside on a system and further comprising: scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations. Furthermore, Reitmeier et al. discloses: a subset of available memory locations are located outside file system locations (Paragraph 18, Lines 9-10, distributed on a DVD-ROM).

As per **claims 18 and 105**, rejected as applied to claims 15 and 102. The combined references Reitmeier et al., Weidong and Jensen et al. substantially teach the memory locations reside on a system and further comprising: scanning the system to determine available memory locations; selecting target memory locations within the

available memory locations at which to store the modified data; and storing the modified data at the target memory locations. Furthermore, Jensen et al. discloses: generating a map of the target memory locations (Column 12, Lines 50-52). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Weidong in order to allow the operating system to locate files.

As per **claims 19 and 106**, rejected as applied to claims 18 and 105. The combined references Reitmeier et al., Weidong and Jensen et al. substantially teach generating a map of the target memory locations. Furthermore, Jensen et al. discloses: storing the map of target memory locations at the target memory locations (Column 12, Lines 1-8, Lines 41-44). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Weidong in order to allow the operating system to locate files.

As per **claims 21 and 108**, rejected as applied to claims 1 and 89. The combined references Reitmeier et al. and Weidong substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; and storing the modified data at predetermined memory locations; encrypting the modified data and storing the encrypted modified data;

encrypting the modified data with an encryption key; encrypting the encryption key; storing the encryption key with the encrypted modified data at the predetermined memory locations; and partitioning the encryption key among the encrypted modified data. The combined teachings of Reitmeier et al. and Weidong do not explicitly disclose the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents. However, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents (file allocation table, Fig. 2B column 6, lines 7-12). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Weidong in order to allow the operating system to locate files.

As per **claims 22 and 109**, rejected as applied to claims 1 and 89. The combined references Reitmeier et al. and Weidong substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; and storing the modified data at predetermined memory locations; encrypting the modified data and storing the encrypted modified data;

encrypting the modified data with an encryption key; encrypting the encryption key; storing the encryption key with the encrypted modified data at the predetermined memory locations; and partitioning the encryption key among the encrypted modified data. The combined teachings of Reitmeier et al. and Weidong do not explicitly disclose the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents. However, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents (Fig. 2B Column 6, Lines 7-12 FAT). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Weidong in order to allow the operating system to locate files.

As per **claims 23 and 110**, rejected as applied to claims 1 and 89. The combined references Reitmeier et al. and Weidong substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; and storing the modified data at predetermined memory locations; encrypting the modified data and storing the encrypted modified data;

encrypting the modified data with an encryption key; encrypting the encryption key; storing the encryption key with the encrypted modified data at the predetermined memory locations; and partitioning the encryption key among the encrypted modified data. The combined teachings of Reitmeier et al. and Weidong do not explicitly disclose the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents. However, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (Fig. 7B Column 6, Lines 7-12). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Weidong in order to allow the operating system to locate files.

As per **claim 24**, rejected as applied to claim 23. The combined references Reitmeier et al., Weidong and Jensen et al. substantially teach the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of

contents. Furthermore, Reitmeier et al. discloses: if an authorized access of a file replaced by the modified data is determined, the file is accessed (Paragraph 18, Lines 13-16).

6. **Claims 27, 28, 113, 114, 159** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Weidong (U.S. Patent No. 6,819,766) in further view of Xu et al. (US Pub. No. 2006/0053307)

As per **claim 159**, Reitmeier et al. discloses: a system for preventing unauthorized use of digital content data in a system having memory locations wherein the system enables a user to select from a plurality of tool modules, each module providing a service for protecting digital content from unauthorized use such that a user can protect digital content (figure 1, [0021], where the user (provider) has configuration options to choose from); modules that perform functions selected from the group of functions of interleaving; tokenization (Paragraph 29-31 Paragraph 57, encryption in electronic codebook mode). Reitmeier et al. does not explicitly teach translocation; shimming. However, Weidong discloses: translocation; shimming (Column 3, Lines 18-29, segmenting into binary representation at locations determined by the set of indices). Weidong further provides the motivation that this method is capable of encryption key management without requiring security infrastructure such as a key distribution center or a certificate authority (Column 2, Lines 30-33). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Weidong in conjunction with the teachings of Reitmeier et al. for the benefit

of managing encryption keys for encrypted data without requiring a security infrastructure. The combined references Reitmeier et al. and Weidong doe not explicitly disclose obfuscation; saturation and assassination. However, Xu et al. discloses: obfuscation; saturation and assassination (Paragraph 11-Paragraph 13, obfuscation upon disassembly). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the combined teachings of Reitmeier et al. and Weidong for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claims 27 and 113**, rejected as applied to claims 26 and 112. The combined references Reitmeier et al. and Weidong substantially teach modifying the data segments with second data comprises tokenizing the data segments with token data. The combined references Reitmeier et al. and Weidong do not explicitly teach the token data comprises lexical equivalents of assembly language commands. However, Xu et al. discloses: the token data comprises lexical equivalents of assembly language commands (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code

which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the combined teachings of Reitmeier et al. and Weidong for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claims 28 and 114**, rejected as applied to claims 27 and 113. The combined references Reitmeier et al., Weidong and Xu et al. substantially teach the token data comprises lexical equivalents of assembly language commands. Furthermore, Xu et al. discloses: the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access (disassembly) (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the combined teachings of Reitmeier et al. and Weidong for the benefit of deterring unwanted parties from making copies of an original

author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

7. **Claims 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 85, 86, 87, 115, 116, 118, 119, 120, 121, 123, 124, 125, 155, 156, 157, 161, 162, 163, 164, 165, 166, 180, 181, 182, 183** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Jensen et al. (US Patent No. 5,930,828).

As per **claim 29**, Reitmeier et al. discloses: subdividing the digital content data into data segments ([0023]); modifying the data segments with second data to generate modified data ([0029]); storing the modified data at the target memory locations ([0036]), and wherein a subset of the available memory locations are located outside file system locations (Paragraph 18, Lines 13-19 DVD-ROM). Reitmeier et al. does not teach scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data. Jensen et al. teaches scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use

the memory scanning and targeting of Jensen et al. with the method of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claims 85**, Reitmeier et al. discloses: storing the digital content data at the target memory locations ([0036]); wherein a subset of the available memory locations are located outside file system locations (Paragraph 18, Lines 13-16 DVD-ROM). Reitmeier et al. do not teach scanning or selecting memory locations. Reitmeier et al. does not explicitly teach scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data. Jensen et al. teach scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanning and targeting of Jensen et al. with the method of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claim 115** Reitmeier et al. discloses: means for subdividing the digital content data into data segments (figure 1, item 110A, [0023]; means for modifying the data segments with second data to generate modified data (figure 1, item 130, [0029]); and a storage unit for storing the modified data at the target memory locations (figure 1,

item 155, [0036]); wherein a subset of the available memory locations are located outside file system locations (Paragraph 18, Lines 13-16 DVD-ROM). Reitmeier et al. does not explicitly teach means for scanning the system to determine available memory locations and a selector for selecting target memory locations within the available memory locations at which to store data. Jensen et al. teach means for scanning the system to determine available memory locations and a selector for selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanning means and selector of Jensen et al. with the system of Reitmeier to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claim 155**, Reitmeier et al. discloses: a storage unit for storing the digital content data at the target memory locations (figure 1, item 155, [0035], [0036]), wherein a subset of the available memory locations are located outside file system locations (Paragraph 18, Lines 13-16 DVD-ROM). The system of Reitmeier et al. does not teach a scanner for scanning the system to determine available memory locations based on a file system identifying locations of files on the system and a means for selecting target memory locations within the available memory locations at which to store the digital content data. Jensen et al. teach a scanner for scanning the system to determine

available memory locations based on a file system identifying locations of files on the system and a means for selecting target memory locations within the available memory locations at which to store the digital content data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanner and selecting means of Jensen et al. with the system of Reitmeier to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claim 161**, Reitmeier et al. discloses: subdividing the digital content data into data segments ([0023]); modifying the data segments with second data to generate modified data ([0029]); storing the modified data at the target memory locations ([0036]) and wherein, if an authorized access of a file replaces by the modified data is determined, the file is accessed (Paragraph 18, Lines 13-16). Reitmeier et al. does not explicitly teach wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents. Jensen et al. discloses: wherein the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (Column 6, Lines 7-12). Jensen et al.

further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Weidong in order to allow the operating system to locate files.

As per **claim 180**, Reitmeier et al. discloses: a subdividing unit for subdividing the digital content data into data segments ([0023]); a modification unit for modifying the data segments with second data to generate modified data ([0029]); a storage unit for storing the modified data at the target memory locations ([0036]) and wherein a subset of the available memory locations are located outside file system locations (Paragraph 18, Lines 13-19 DVD-ROM). Reitmeier et al. do not teach a scanner for scanning the system to determine available memory locations and a selector for selecting memory locations and wherein a subset of the available memory locations are located outside file system locations (Paragraph 18, Lines 13-16 DVD-ROM). Jensen et al. teaches scanning the system to determine available memory locations and selecting target memory locations within the available memory locations at which to store data (column 12, lines 13-19, 27-31). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory scanning and targeting of Jensen et al. with the method of Reitmeier et al. to store data

in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claim 30, 86, 116 and156**, rejected as applied to claim 29, 85, 115 and 155. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Jensen et al. discloses: subset of available memory locations are located within file system locations (Column 3, Lines 55-61). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the teachings of Jensen et al. with the teachings of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claim 32 and 118**, rejected as applied to claim 29 and 115. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at

which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Jensen et al. discloses: generating a map of the target memory locations (Column 12, Lines 50-52). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the teachings of Jensen et al. with the teachings of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claims 33 and 119**, rejected as applied to claims 32 and 118. The combined references Reitmeier et al. and Jensen et al. substantially generating a map of the target memory locations. Furthermore, Jensen et al. discloses: storing the map of target memory locations at the target memory locations. Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the teachings of Jensen et al. with the teachings of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claim 34**, rejected as applied to claim 29. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Reitmeier discloses: data types selected from a group consisting of audio, video, documents, text and software (Paragraph 16).

As per **claims 35 and 162**, rejected as applied to claim 29 and 161. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Reitmeier et al. discloses: the data segments are of a variable length (Paragraph 29).

As per **claims 36 and 163**, rejected as applied to claim 29 and 161. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory

locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Reitmeier et al. discloses: the second data comprises a randomly generated data stream (Paragraph 29).

As per **claims 37 and 164**, rejected as applied to claim 29 and 161. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Reitmeier et al. discloses: the second data comprises portions of the digital content data (Paragraph 29).

As per **claim 38 and 120**, rejected as applied to claim 29 and 115. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file

system locations. Furthermore, Reitmeier et al. discloses: encrypting the modified data and storing the encrypted modified data (Paragraph 36).

As per **claim 39 and 121**, rejected as applied to claim 38 and 120. The combined references Reitmeier et al. and Jensen et al. substantially teach encrypting the modified data and storing the encrypted modified data. Furthermore, Reitmeier et al. discloses: encrypting the modified data with an encryption key (Paragraph 31 Paragraph 57).

As per **claim 43**, rejected as applied to claim 29. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Jensen et al. discloses: the predetermined memory locations are selected as the locations at which the digital content data was originally stored. (Column 12, lines 46-49). ). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the teachings of Jensen et al. with the teachings of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

As per **claims 44**, rejected as applied to claim 29. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations.. Furthermore, Reitmeier et al. discloses: first and second digital content data and wherein the predetermined memory locations are selected as combinations of the locations at which the first and second digital content data were originally stored (Paragraph 29).

As per **claims 45**, rejected as applied to claim 29. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Reitmeier et al. discloses: generating a map of locations at which the modified data is stored (Paragraph 18, index table).

As per **claims 46**, rejected as applied to claims 45. Furthermore, Reitmeier et al. discloses: storing the map of locations at the predetermined memory locations (Paragraph 18 and Paragraph 36).

As per **claims 47**, rejected as applied to claim 29. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations.. Furthermore, Reitmeier et al. discloses: retrieving the modified data from the predetermined memory locations; and de-interleaving the data segments based on the second data to generate original digital content data (Fig 4, Paragraph 46).

As per **claims 48, 123, 165 and 181**, rejected as applied to claim 29, 115, 161 and 180. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents (file allocation table, Fig. 2B column 6, lines 7-12).

Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the teachings of Reitmeier et al. in order to allow the operating system to locate files.

As per **claims 49, 124, 166 and 182**, rejected as applied to claim 29, 115, 161 and 180. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents (Fig. 2B Column 6, Lines 7-12 FAT). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the teachings of Reitmeier et al. in order to allow the operating system to locate files.

As per **claims 50, 125 and 183**, rejected as applied to claim 29,115 and 180. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (Fig. 7B Column 6, Lines 7-12). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the teachings Reitmeier et al. in order to allow the operating system to locate files.

As per **claim 51**, rejected as applied to claim 50. The combined references Reitmeier et al. and Jensen et al. substantially teach the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents. Furthermore, Reitmeier et al. discloses: if an authorized access of a file

replaced by the modified data is determined, the file is accessed (Paragraph 18, Lines 13-16).

As per **claims 52**, rejected as applied to claim 29. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. Furthermore, Reitmeier et al. discloses: modifying the data segments comprises interleaving the data segments with the second data to generate interleaved data (Paragraph 57).

As per **claim 53**, rejected as applied to claim 29. The combined references Reitmeier et al. and Jensen et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; scanning the system to determine available memory locations; selecting target memory locations within the available memory locations at which to store the modified data; and storing the modified data at the target memory locations, wherein a subset of the available memory locations are located outside file system locations. . Furthermore, Reitmeier et al. discloses: modifying the data segments with second data comprises tokenizing the data segments with token data (Paragraph 31, encryption in electronic codebook mode).

As per **claims 87 and 157**, rejected as applied to claims 85 and 115. The combined references Reitmeier et al. and Jensen et al. substantially teach scanning the system to determine available memory locations based on a file system identifying locations of files on the system; selecting target memory locations within the available memory locations at which to store the digital content data; and storing the digital content data at the target memory locations, wherein a subset of the available memory locations are located outside the file system locations. Furthermore, Jensen et al. discloses: subset of available memory locations are located between files identified by the file system locations (Column 3, Lines 55-61). Furthermore, Jensen et al. discloses: subset of available memory locations are located within file system locations (Column 3, Lines 55-61). Jensen et al. further provide the motivation that this method minimizes fragmentation of free space on a disk storage device, which increases computer system efficiency (column 2, lines 32-34, 44-48). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the teachings of Jensen et al. with the teachings of Reitmeier et al. to store data in a way that minimizes free space fragmentation and therefore increases program efficiency.

8. **Claims 40, 41, 42 and 122** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Jensen et al. (US Patent No. 5,930,828) in further view of Weidong (U.S. Patent No. 6,819,766).

As per **claims 40 and 122**, rejected as applied to claims 39 and 121. The combined references Reitmeier et al. and Jensen et al. substantially teach encrypting the modified data with an encryption key. The combined references do not explicitly teach encrypting the encryption key. However, Weidong discloses: encrypting the encryption key (Column 2, Lines 48). Weidong further provides the motivation that this method is capable of encryption key management without requiring security infrastructure such as a key distribution center or a certificate authority (Column 2, Lines 30-33). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Weidong in conjunction with the combined teachings of Reitmeier et al. and Jensen et al. for the benefit of managing encryption keys for encrypted data without requiring a security infrastructure.

As per **claim 41**, rejected as applied to claim 40. The combined references Reitmeier et al., Jensen et al. and Weidong substantially teach encrypting the encryption key. Furthermore, Weidong discloses: storing the encryption key with the encrypted modified data at the predetermined memory locations (Column 2, Lines 50-61). Weidong further provides the motivation that this method is capable of encryption key management without requiring security infrastructure such as a key distribution center or a certificate authority (Column 2, Lines 30-33). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Weidong in conjunction with the combined teachings of Reitmeier et al. and Jensen et al. for the benefit of managing encryption keys for encrypted data without requiring a security infrastructure.

As per **claim 42**, rejected as applied to claim 41. The combined references Reitmeier et al., Jensen et al. and Weidong substantially teach storing the encryption key with the encrypted modified data at the predetermined memory locations. Furthermore, Weidong discloses: partitioning the encryption key among the encrypted modified data (inserting segments into the encrypted data (Column 2, Lines 50-51). Weidong further provides the motivation that this method is capable of encryption key management without requiring security infrastructure such as a key distribution center or a certificate authority (Column 2, Lines 30-33). Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to use the teachings of Weidong in conjunction with the combined teachings of Reitmeier et al. and Jensen et al. for the benefit of managing encryption keys for encrypted data without requiring a security infrastructure.

9. **Claims 54 and 55** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Jensen et al. (US Patent No. 5,930,828) in further view of Xu et al. (US Pub. No. 2006/0053307).

As per **claim 54**, rejected as applied to claim 53. The combined references Reitmeier et al. and Jensen et al. substantially teach modifying the data segments with second data comprises tokenizing the data segments with token data. The combined references Reitmeier et al. and Jensen et al. do not explicitly teach the token data comprises lexical equivalents of assembly language commands. Xu et al.

discloses: the token data comprises lexical equivalents of assembly language commands (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the combined teachings of Reitmeier et al. and Jensen et al. for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claims 55**, rejected as applied to claims 54. The combined references Reitmeier et al., Jensen et al. and Xu et al. substantially teach the token data comprises lexical equivalents of assembly language commands. Furthermore, Xu et al. discloses: the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access (disassembly) (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art

at the time the invention was made to use the teachings of Xu et al. in conjunction with the combined teachings of Reitmeier et al. and Jensen et al. for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

10. **Claims 56, 57, 59, 60, 61, 62, 63, 126, 127, 129, 130, 132, 133, 167, 168, 169, 170, 171, 175 and 176** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Xu et al. (US Pub. No. 2006/0053307).

As per **claim 56**, Reitmeier et al. discloses: modifying the digital content data with saturation data to generate modified data ([0029]); and storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data ([0036]). Reitmeier et al. does not explicitly teach determining whether an unauthorized attempt at accessing the digital content data occurs; and in the event of unauthorized access, generating saturation traffic on the system to deter unauthorized activity. However, Xu et al. discloses: determining whether an unauthorized attempt at accessing the digital content data occurs (Paragraph 11); and in the event of unauthorized access, generating saturation traffic on the system to deter unauthorized activity (Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code

which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the teachings of Reitmeier et al. for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claim 126**, Reitmeier et al. discloses: a modification unit for modifying the digital content data with saturation data to generate modified data ([0029]); and a storage unit for storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data ([0036]). Reitmeier et al. does not explicitly teach means for determining whether an unauthorized attempt at accessing the digital content data occurs; and in the event of unauthorized access, generating saturation traffic on the system to deter unauthorized activity. However, Xu et al. discloses: means for determining whether an unauthorized attempt at accessing the digital content data occurs (Paragraph 11); and in the event of unauthorized access, generating saturation traffic on the system to deter unauthorized activity (Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph

11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the teachings of Reitmeier et al. for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claim 167**, Reitmeier et al. discloses: subdividing the digital content data into data segments (Paragraph 23); modifying the data segments with second data to generate modified data (Paragraph 29); and storing the modified data at predetermined memory locations (Paragraph 36). Reitmeier et al. does not explicitly teach wherein modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands. However, Xu et al. discloses: wherein modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the teachings of Reitmeier et al. for the

benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claim 175**, Reitmeier et al. discloses: a subdividing unit for subdividing the digital content data into data segments (Paragraph 23); a modification unit for modifying the data segments with second data to generate modified data (Paragraph 29); and a storage unit for storing the modified data at predetermined memory locations (Paragraph 36). Reitmeier et al. does not explicitly teach wherein the modification unit modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands. However, Xu et al. discloses: wherein the modification unit modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the teachings of Reitmeier et al. for the benefit of deterring unwanted parties from making copies of an

original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claims 57 and 127**, rejected as applied to claims 56 and 126. The combined references Reitmeier et al. and Xu et al. substantially teach a modification unit for modifying the digital content data with saturation data to generate modified data; and a storage unit for storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data; and means for determining whether an unauthorized attempt at accessing the digital content data occurs; and in the event of unauthorized access, generating saturation traffic on the system to deter unauthorized activity. Furthermore, Reitmeier et al. discloses: subdividing the digital content data into data segments and modifying the data segments (Paragraph 23-29).

As per **claims 59 and 129**, rejected as applied to claims 56 and 126. The combined references Reitmeier et al. and Xu et al. substantially teach a modification unit for modifying the digital content data with saturation data to generate modified data; and a storage unit for storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data; and means for determining whether an unauthorized attempt at accessing the digital content data occurs; and in the event of unauthorized access, generating saturation traffic on the system to deter unauthorized activity. Furthermore, Xu et al. discloses: the saturation traffic comprises system commands that burden system resources (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of

hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the teachings of Reitmeier et al. for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claims 60 and 130**, rejected as applied to claims 59 and 129. The combined references Reitmeier et al. and Xu et al. substantially teach he saturation traffic comprises system commands that burden system resources. Furthermore, Xu et al. disclose: the system commands are generated as a function of activity utilizing the system resources subject to the unauthorized access (disassembly Paragraph 11-13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the teachings of Reitmeier et al. for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the

software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claims 62 and 132**, rejected as applied to claims 56 and 126. Furthermore, Reitmeier et al. discloses: interleaving the digital content data with second data to generate interleaved data (Paragraph 23-29 and Paragraph 57).

As per **claims 63 and 133**, rejected as applied to claims 56 and 126. Furthermore, Reitmeier et al. discloses: tokenizing the digital content data with token data (Paragraph 31, encryption).

As per **claims 168 and 176**, rejected as applied to claims 167 and 175. The combined references Reitmeier et al. and Xu et al. substantially teach subdividing the digital content data into data segments; modifying the data segments with second data to generate modified data; and storing the modified data at predetermined memory locations, wherein modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands. Furthermore, Xu et al. discloses: the lexical equivalents are consumed by a system interpreter, in turn generating alternative assembly language commands selected to obfuscate the digital content data in the event of an unauthorized access (disassembly) (Paragraph 11-Paragraph 13). Xu et al. further provides motivation that this method is capable of hiding, masking or other wise obfuscating original software code which helps thwart unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines

1-7). Therefore it would have been obvious to one with ordinary skill in eth art at the time the invention was made to use the teachings of Xu et al. in conjunction with the teachings of Reitmeier et al. for the benefit of deterring unwanted parties from making copies of an original author's software, obtaining valuable information from the software for purposes of breaking into the program, stealing secrets, etc...(Paragraph 11, Lines 1-7).

As per **claims 169, 170 and 171**, rejected as applied to claim 167. Reitmeier et al. discloses: the data segments are of a variable length (Paragraph 29); the second data comprises a randomly generated data stream (Paragraph 29); the second data comprises portions of the digital content data (Paragraph 29).

11. **Claims 172, 173, 174, 177, 178 and 179 are** rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Xu et al. (US Pub. No. 2006/0053307) in further view of Jensen et al. (US Patent No. 5,930,828).

As per **claims 172 and 177**, rejected as applied to claims 167 and 175. The combined references Reitmeier et al. and Xu et al. substantially teach a subdividing unit for subdividing the digital content data into data segments; a modification unit for modifying the data segments with second data to generate modified data; and a storage unit for storing the modified data at predetermined memory locations, wherein the modification unit modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical

equivalents of assembly language commands. The combined references Reitmeier et al. and Xu et al. do not explicitly teach the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents. However, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are between memory locations used by files stored on the system, as identified by the table of contents (file allocation table, Fig. 2B column 6, lines 7-12). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Xu et al. in order to allow the operating system to locate files.

As per **claims 173 and 178**, rejected as applied to claims 167 and 175. The combined references Reitmeier et al. and Xu et al. substantially teach a subdividing unit for subdividing the digital content data into data segments; a modification unit for modifying the data segments with second data to generate modified data; and a storage unit for storing the modified data at predetermined memory locations, wherein the modification unit modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands. The combined references Reitmeier et

al. and Xu et al. do not explicitly teach the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents. However, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system, and wherein a subset of the memory locations used for storing the modified data are exclusive of memory locations of files stored on the system, as identified by the table of contents (Fig. 2B Column 6, Lines 7-12 FAT). Jensen et al. further provide the motivation that this allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Xu et al. in order to allow the operating system to locate files.

As per **claims 174 and 179**, rejected as applied to claims 167 and 175. The combined references Reitmeier et al. and Xu et al. substantially teach a subdividing unit for subdividing the digital content data into data segments; a modification unit for modifying the data segments with second data to generate modified data; and a storage unit for storing the modified data at predetermined memory locations, wherein the modification unit modifying the data segments with second data comprises tokenizing the data segments with token data and wherein the token data comprises lexical equivalents of assembly language commands. The combined references Reitmeier et al. and Xu et al. do not explicitly teach the memory locations reside on a system and

wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents. However, Jensen et al. discloses: the memory locations reside on a system and wherein a table of contents identifies files stored on the system and identifies memory locations at which the files are stored, and wherein the modified data are stored at memory locations occupied by the files, as identified by the table of contents (Fig. 7B Column 6, Lines 7-12). Jensen et al. further provide the motivation that this method allows the operating system to find a file and all its parts (column 6, lines 7-12). It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the memory table of contents of Jensen et al. with the combined references Reitmeier et al. and Xu et al. in order to allow the operating system to locate files.

12. **Claims 131 and 61** are rejected under 35 U.S.C. 103(a) as being unpatentable over (Reitmeier et al., US Pub. No. 2002/0003881) in view of Xu et al. (US Pub. No. 2006/0053307) in further view of Atallah et al. (US Pub. No. 2006/0031686).

As per **claim 61 and 131**, rejected as applied to claims 56 and 126. The combined references Reitmeier et al. and Xu et al. substantially teach a modification unit for modifying the digital content data with saturation data to generate modified data; and a storage unit for storing the modified data at predetermined memory locations on the system to deter unauthorized access of the digital content data; and means for determining whether an unauthorized attempt at accessing the digital content data

occurs; and in the event of unauthorized access, generating saturation traffic on the system to deter unauthorized activity. The combined references Reitmeier et al. and Xu et al. do not explicitly teach determining whether an unauthorized attempt at accessing the digital content data occurs comprises monitoring activity of the system hosting the digital content data and determining whether the activity is inconsistent with the type of digital content data being hosted. However, Atallah et al. discloses: determining whether an unauthorized attempt at accessing the digital content data occurs comprises monitoring activity of the system hosting the digital content data and determining whether the activity is inconsistent with the type of digital content data being hosted (Paragraph 154-156). Atallah et al. further provides motivation that method provides protection of host application code by installing a plurality of guards that cooperatively protect the host application code (abstract). Therefore, It would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to use the teaching sof Atallah et al. in conjunction with the combined references Reitmeier et al. and Xu et al. for the benefit of protecting host application code.

***Conclusion***

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Saoussen Besrour whose telephone number is 571-272-6547. The examiner can normally be reached on M-F 8:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SB
November 30, 2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Continuation of Disposition of Claims: Claims pending in the application are 1-5,11-30,32,57,59-63,85-87,89-92,98-116,118-127,129-133,155-157,159 and 161-183.